Assessment of Student Vulnerability on the Download of Malware Disguised as Cracked Software

Eric Blancaflor, Christer John Esguerra, Dan Christopher Fandiño, Angelo Luisse Gonzales, Bryelle Nisperos, and Luis Angelo Pono
School of Information Technology
Mapua University
Makati, Philippines
ebblancaflor@mapua.edu.ph, christerjohnesguerra@gmail.com, dan.fandino04@gmail.com, gelgonzales32800@gmail.com, brylltcn@gmail.com, luisangelopono@gmail.com

Abstract
Users are prone to cyberattacks due to unlicensed software which may contain malicious entities. This study then assesses student vulnerability on the download of a malware disguised as cracked software through social engineering. Furthermore, the study assesses the level of security their browsers have when met with a malicious file. This study uses a quantitative method. The study's participants, college students, were given an instruction to download the software which is Adobe Photoshop without any indication that it contains malicious software located in a batch (.bat) file. Based on the data collected, the researchers concluded that most of the students are susceptible to the vulnerability of downloading a cracked software, Adobe Photoshop carrying a malicious software.

Keywords
student vulnerability, social engineering, browser, Adobe Photoshop, batch, cracked software

1. INTRODUCTION

Software applications, through the years, have integrated itself to the day to day lives of people. The aforementioned could be in the form of video games, browsers and the likes, entertaining its users. It could also be a tool, aiding them in different areas such as word processing, photo editing, calculating and the likes. Students, especially in the college level, have an escalated need for this software. However, these software applications are in the price range that students could not normally afford. Microsoft Office 365 Personal is currently priced at around $70. You can subscribe to Adobe Photoshop at $21 a month. PHStat, a statistical analysis tool is priced around $10. These prices may be too heavy for a student relying on allowance to handle. This is why they rely on pirated software. Pirated software is software that is copied and distributed for free against the will of the developer. The Business Software Alliance conducted a study and found out that computer users all over the world have the tendency to install unlicensed computer software. Malicious software can be disguised as part of the installation files or the license activator. A study conducted by Munasinghe and Pemarathna examines and identifies the intentions of students when it comes to using pirated software. The researchers concluded that computer experience, attitudes, awareness of software and social influence pushes students to use pirated software, with moral obligation being neglected. It implies that students need the software but cannot afford it. They can also be motivated by peers (Pemarathna et al. 2017). These malicious files could be in forms that normal users wouldn't usually anticipate. These viruses would then go on wrecking damage to the user's device. This is dangerous because these files contain line commands that attackers could utilize to do activity that may bring harm to users. Malicious .bat files can be disguised as crack files for software such as Adobe Photoshop. As shown in the Conceptual Framework of the Study in Figure 1, this study then assesses the awareness of users, particularly college students, when it comes to the vulnerabilities of installing pirated software. Furthermore, this would also assess the level of security their browsers have when met with a malicious file.

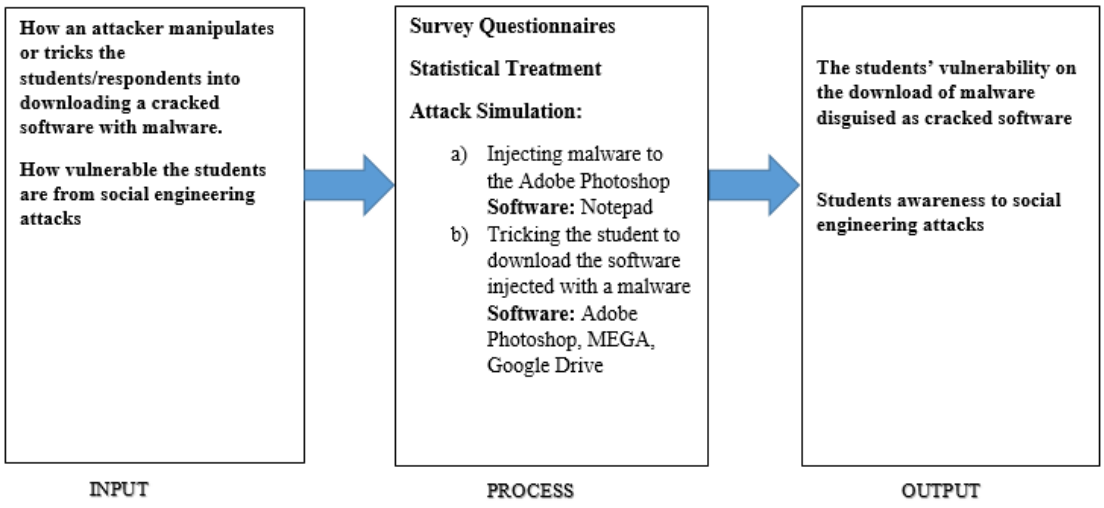

Figure 1. The Conceptual Framework of the Study

1.1 Objectives

A case study designed to assess student vulnerability on the download of a malware disguised as cracked software through social engineering had the following general and specific objectives:

General Objective: To assess student vulnerability in social engineering attack by tricking them to download a cracked software injected with a malware

Specific Objectives:

- To determine if the students know how to examine files they've downloaded in the internet
- To assess the awareness of the students with regards to the social engineering attack
- To analyze the impact of subscription fees in programs needed by students that make them settle in cracked programs on torrents and other websites

2. Literature Review

Consumer digital piracy behaviour among youths: insights from Indonesia by Arli, D. and Tjiptono, F.(2016)

Piracy is one of the problems that is persistent on the internet that is being used by many for various reasons. Many perceive it to be illegal and a method that should not be tolerated but it is still considered as widespread. The reason for its widespread use varies from person to person and with that, many researchers have conducted studies based on this. One study focuses on the attitude of people in Indonesia when it comes to piracy and their intention or reasoning behind on why they are committing this act. According to the study, Indonesia is a country that has a large population and with it, one of the highest digital piracy rates. In order to analyze this, the researchers used a convenience sampling approach in which 400 questionnaires were given to college students in one private university and in one public university in Yogyakarta, Indonesia. The questionnaires are primarily composed of questions with regards to digital piracy and the consumers' intention behind it. The findings showed that the consumers were greatly influenced by their attitude towards digital piracy in which it is considered as heavily convenient rather than buying legal or licensed software. Also, legal consequences and punishment were not a huge factor or predictors to the attitude of the consumers. Overall, the study showed that many people have little to no fear in regards to the punishment that they might receive when committing the act of piracy and that a huge factor of it comes from their attitude towards privacy.

Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach Ullah. et al. (2019)

The Internet of Things is widely regarded as a new way to connect various systems with each other through the internet. Each of these systems or devices are identified through the use of Radio Frequency Identifier tags and can then be controlled remotely. In line with this, many cyber-attacks can infiltrate various IoT systems. Malware, viruses, worms and other forms of attacks can be present in these systems without the user's knowledge. In line with this, the researchers have conducted a study with the purpose of detecting software that is pirated and files that are infected with malware across IoT systems. The researchers used a deep neural network called TensorFlow that is able to detect pirated software with the use of source code plagiarism. The methods used in the network feature the tokenization and weighing feature methods. These are used to filter noisy or unnecessary data along with the ability to zoom each token's importance to the source code plagiarism. The data is then gathered and collected from Google Code Jam with the intent of investigating software piracy. The neural network is also used to detect infections in IoT systems through the process of color image visualization. Findings and results states that the proposed solution that was used to measure threats that are persistent in IoT is better than the state-of-the-art methods. With this, the study conducted stated that even in IoT, pirated software is persistent and becomes a cyber-attack when malware is involved and injected. Proper countermeasures can be used such as the one conducted in the study to prevent the spread of malware in IoT and even in other systems.

Malware in Pirated Software: Case Study of Malware Encounters in Personal Computers by Sikdar et al. (2016)

Pirated software is used by many people all over the world and a huge fraction of personal computers have it installed and running. With this, many people are becoming targets of criminals that uses pirated software that is being installed by a majority of people and bundling it with malware or any other form of malicious or dangerous software. In line with this, a study is conducted with the purpose of quantifying the presence of malware in pirated software that is included in computers that are newly purchased. The study evaluates the malware that is present in the software, which includes its type and location. The results of the study indicated that 63% of the computers used for the study came with malware installed or present. It also showed that Trojans and Hacktools are the most frequently installed malware in the samples used. In line with this, it can be stated that malware in pirated software is not an uncommon occurrence. Various pirated software that is easily accessible online can come with malware, viruses or any other type of dangerous software and many users are unaware of this. The study conducted further proved that even people who are purchasing new computers for themselves are unaware that malware can be located with their newly purchased computers and will later fall victim to various attacks. Awareness and security is always crucial and one must always have this in mind when purchasing computers or downloading software.

3. Methods

Research Design

This study used a quantitative method for the research since it dealt with the analysis of data obtained with the use of a survey after the participants have finished downloading the application.

Research Respondents

The participants were composed of 15 college students who are currently enrolled in the age group of 18-25 years old. The researchers instructed the participants to download the software with either Google Drive or Mega and is instructed to take the survey after they installed the software. The researchers used snowball purposive sampling in this study.

Research Instrument

The participants were given an instruction to download the software which is Adobe Photoshop without any indication that it contains malicious software. The participants will then be instructed to install the software and when successfully installed, will be prompted a warning that the software is malicious and will be instructed to answer a survey questionnaire via the use of Google Forms.

4. Data Collection

Data Gathering

The participants would be given a link pointing towards either Google Drive or Mega and will be instructed to download and install the files. Afterwards the installation will show that the software has a malicious code attached to it by automatically opening notepad and will instruct the user to answer the Google Form. The self-assessment that they inputted would be documented.

Samples and Sampling Techniques

The researchers will be using snowball purposive sampling in this study. Respondents who will be selected in the survey would be students who are acquaintances with the researchers.

Statistical Treatment

The researchers will be using frequency, percentage and mean in representing the set of data, as shown in Table 1. This will be used to compute the scores using a formula and determine the verbal interpretation shown below to each answer in the questionnaire. Thus, it will help conclude the answer to the research question.

$\bar{x} = x_1 \ldots x_n / x_n$

n = the total number of respondents
x = the value of responses
$\bar{x}$ = the mean

% = f / n * 100

n = the total number of respondents
% = is the percentage
f = is the frequency of response

Weighted Mean		
Scale	***Range-Value***	***Verbal Interpretation***
5	4.50 – 5.00	Highly Acceptable
4	3.50 – 4.49	Acceptable
3	2.50 – 3.49	Moderately Acceptable
2	1.50 – 2.49	Fairly Acceptable
1	1.00 – 1.49	Not Acceptable

Table 1. Weighted Mean

5. Results and Discussion

5.1 Numerical Results

For the first question, the researchers asked the respondents on what browser did they use to download the .rar file with the malicious batch file. 14 of the respondents have used Google Chrome to download the file while 1 used Brave Browser. In the second question, the respondents were asked about the website which they used to download the .rar file. 13 of the respondents downloaded the file from Google Drive while 2 downloaded it from Mega. For the third question, the researchers asked the respondents if they have read and followed the readme file that was included in the .rar file that contains the details on how to install the software. 13 of the respondents followed the readme file while 2 chose to not follow the readme file and just proceed with the installation. For the fourth question, the respondents were asked about the file detection of their respective browsers and if it detected any harmful files or entities in the .rar file. 15 of the respondents answered no wherein their browser did not detect any harmful files. For the fifth question, the respondents were asked if they have an antivirus installed in their system. All 15 of the respondents answered that they indeed have an antivirus installed in their own systems. In continuation for research question #5, the respondents that stated they have an antivirus installed were asked on what specific antivirus they are currently operating. 1 answered Avast, 2 answered Avira, 1 answered Malwarebytes, 1 answered McAfee, 1 answered Norton and 7 answered Microsoft Windows Defender. Also in continuation on the 5th research question, the respondents were asked if their specific antivirus detected any harmful files or entities in the downloaded .rar file. 12 of the respondents stated that their own antivirus did not detect any harmful or malicious entities in their downloaded file while 3 of the respondents have an antivirus that was able to detect the malicious file included in the downloaded

software. For the 6th research question, the researchers asked the respondents if they checked all the files in the installation folder, both the main and sub folder, before installing the software. 9 of the respondents answered that they checked all the files while 6 did not check the files in the installation folder before installing the software.

For the 7th research question and the foregoing questions, the questions are based on the experience of the respondents and their awareness when it comes to malicious software that can be downloaded from the internet. The questions were answered with a 5-point Likert scale where 5 is strongly agree, 4 is agree, 3 is neutral, 2 is disagree and 1 is strongly disagree.

In the 7th research question, the respondents were asked about the need of the respondents to access paid software. 11 of the respondents agreed that they usually need paid software to use where 5 strongly agreed. 2 answered neutral while 2 disagreed. In the 8th research question, the respondents were asked if they buy the software that they need. 8 disagreed overall wherein 5 of the respondents strongly disagreed, 2 answered neutral while 5 agreed wherein 1 strongly agreed. In the 9th research question, the respondents were asked if they download software from the internet if they cannot afford to buy it. 12 respondents agreed where 9 of them strongly agreed. 3 respondents disagreed wherein 1 strongly disagreed. In continuation of the previous question, the respondents were asked if they still download from the internet even if they are able to afford the software that they need. 10 of the respondents agreed where 5 strongly agreed. 2 are neutral while 3 disagreed where 1 strongly disagreed. For the 10th research question, the respondents were asked if they frequently use torrent software in order to download the applications or software that they need. 10 of the respondents agreed wherein 6 strongly agreed. 1 is neutral while 4 disagreed. In the 11th research question, the respondents were asked if they have any certain form of awareness when it comes to harmful files that can be included in unlicensed software. All 15 of the respondents agreed where 13 strongly agreed. In the 12th research question, the respondents were asked if they are aware about the concept of social engineering wherein it can be a way to send harmful files to one's system without the user's knowledge. 14 of the respondents agreed where 11 strongly agreed while 1 is neutral.

5.2 Graphical Results

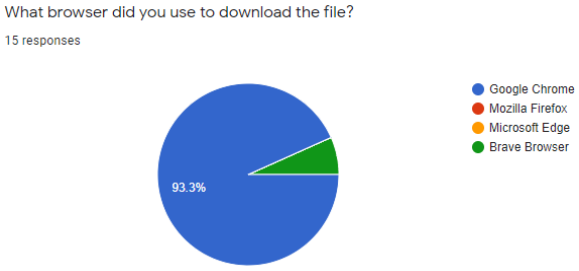

Figure 2. Pie Chart Result of Question #1

As presented in Figure 2, the researchers first asked the respondents which browser the respondents prefer to use in downloading the .rar file. 93.3% of the respondents have used Google Chrome to download the file while 6.7% used Brave Browser. This implies that majority of the respondents prefer using the Google Chrome browser in downloading files.

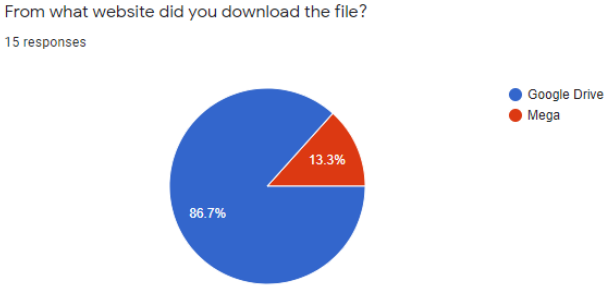

Figure 3. Pie Chart Result of Question #2

In the following question, in Figure 3, the respondents were then asked which website they used to download the .rar file. 86.7% of the respondents downloaded the file from Google Drive while 13.3% downloaded it from Mega. With these results, it is evident that Google Drive is the preferred website for accessing and downloading pirated software rather than Mega.

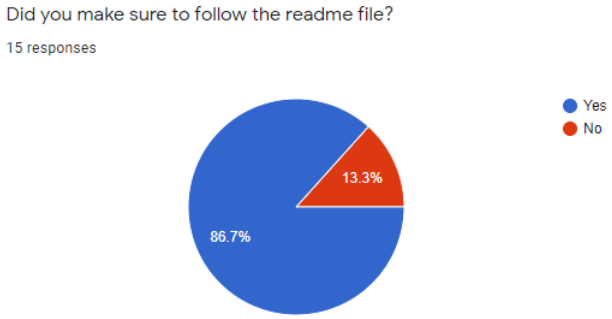

Figure 4. Pie Chart Result of Question #3

Figure 4 asks the respondents if they have read and followed the readme file containing details on the installation. 86.7% of the respondents followed the readme file while 13.3% chose to not follow the readme file and just proceed with the installation. This means that most of the respondents tend to read instructions first before proceeding to the installation process. This shows good practice since it is important to take note of the steps needed to be done to properly install something, rather than installing right away, unaware that something could go wrong.

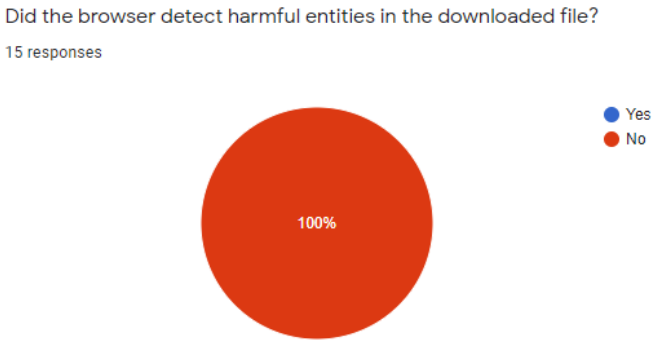

Figure 5. Pie Chart Result of Question #4

Next, in Figure 5, the respondents were asked about the file detection of their respective browsers, and whether it detected any harmful entities in the .rar file or not. All of the respondents' respective browsers did not detect any harmful files. This result states that the respondents' browsers are incapable of detecting the malicious file that was included with the downloaded software they obtained from the internet.

Figure 6. Pie Chart Result of Question #5

The respondents were then asked in Figure 6 if an antivirus is installed in their system. All of the respondents answered that they indeed have an antivirus installed in their own systems. This indicates that the respondents are aware that antiviruses can be helpful in detecting malicious software.

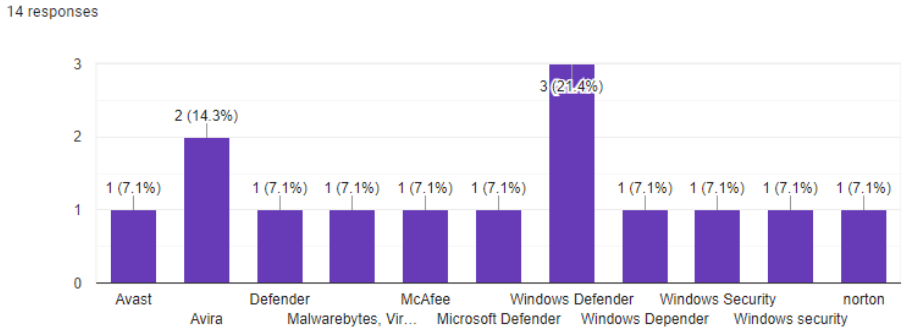

Figure 7. Bar Graph Result of Question #6

As a follow up to the previous question, as shown in Figure 7, the respondents that stated they have an antivirus installed were asked on what specific antivirus they are currently operating. Only 7.1% answered Avast, Malwarebytes, McAfee, and Norton, 14.3% answered Avira, and 49.8% answered Microsoft Windows Defender. This implies that Microsoft Windows Defender, a pre-installed antivirus software among devices running on the Windows platform, is preferred among respondents.

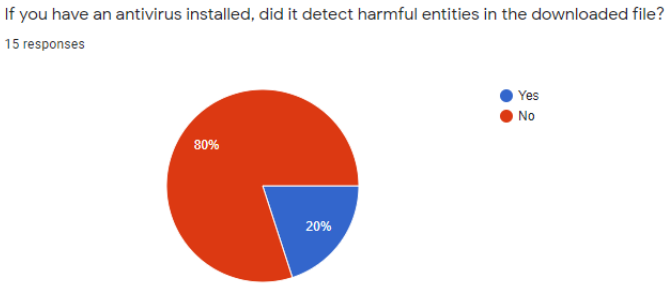

Figure 8. Pie Chart Result of Question #7

In Figure 8, which is related to the 5th question, the respondents were asked if the specific antivirus they used has detected any harmful entities in the .rar file. 80% of the respondents stated that their own antivirus did not detect any harmful or malicious entities in their downloaded file while 20% of the respondents have an antivirus that was able to detect the malicious file included in the downloaded software. This is not a good implication since preferred antivirus applications were not able to detect malicious entities being installed on the device.

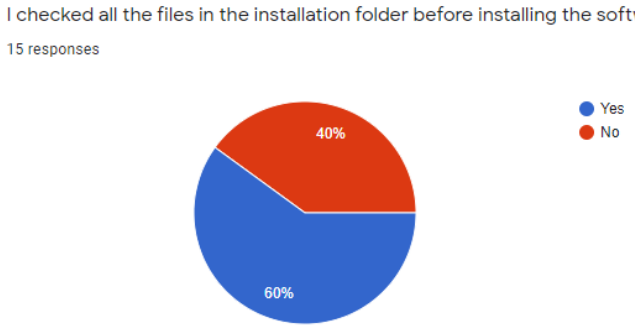

Figure 9. Pie Chart Result of Question #8

The researchers asked in Figure 9 if the respondents checked all the files in the installation folder, before installing the software. 60% of the respondents answered that they checked all the files while 40% did not check the files in the installation folder before installing the software. This indicates that most of the respondents tend to check the files in an installation folder as a sign of caution and as good practice.

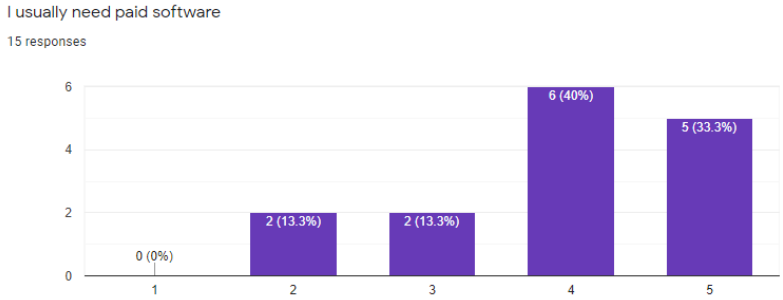

Figure 10. Bar Graph Result of Question #9

As for Figure 10, the respondents were asked about the need of to access paid software. 73.3% of the respondents agreed that they usually need paid software to use where 33.3% strongly agreed. 13.3% answered neutral while 13.3% disagreed. This indicates that majority of the respondents have the need to use paid software either for personal or educational use.

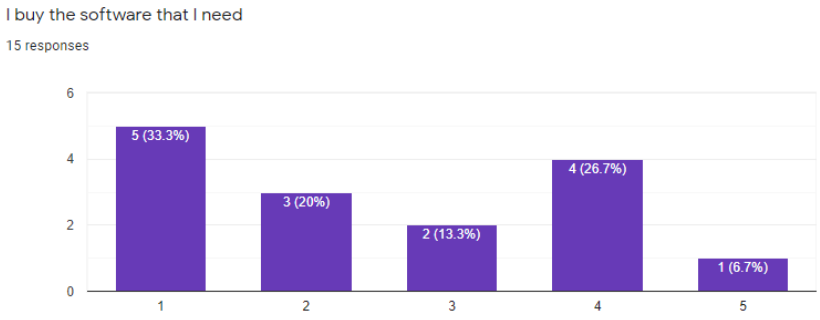

Figure 11. Bar Graph Result of Question #10

Then, in Figure 11, the respondents were asked if they buy the software that they need. 53.3% disagreed overall wherein 33.3% of the respondents strongly disagreed, 13.3% answered neutral while 33.4% agreed wherein 6.7% strongly agreed.

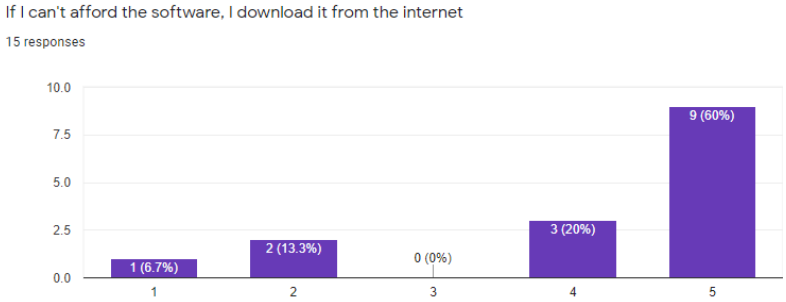

Figure 12. Bar Graph Result of Question #11

For the question presented in Figure 12, the respondents were then asked if they download software from the internet if they cannot afford to buy it. 80% respondents agreed where 60% of them strongly agreed. 20% of the respondents disagreed wherein 6.7% strongly disagreed. These results indicate that majority of the respondents download or pirate software that they need from the internet.

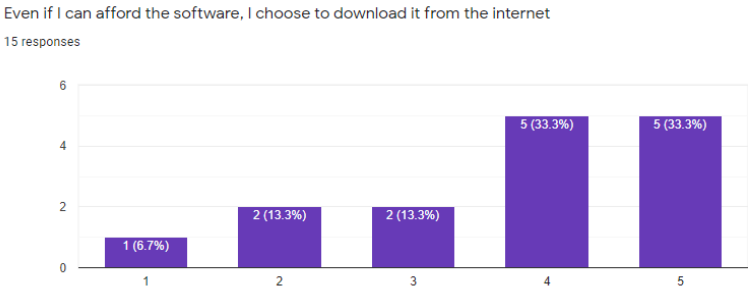

Figure 13. Bar Graph Result of Question #12

As a follow up for the previous question, the respondents were asked in Figure 13 if they still download from the internet even if they are able to afford the software that they need. 66.6% of the respondents agreed where 33.3% strongly agreed. 13.3% are neutral while 20% disagreed where 1 strongly disagreed. These results state that majority of the respondents still prefer to download software that they want or need from the internet rather than paying for said software.

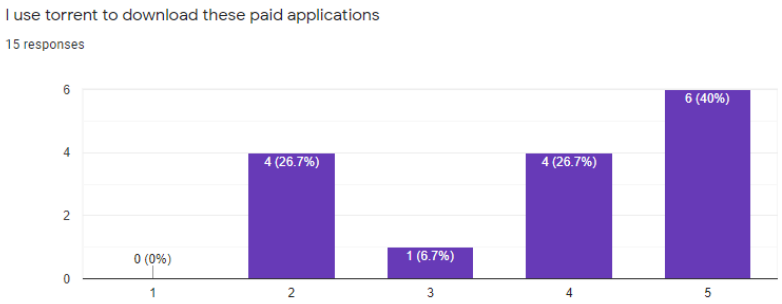

Figure 14. Bar Graph Result of Question #13

Next, in Figure 14, the respondents were asked if they frequently use torrent software in order to download the applications or software that they need. 66.7% of the respondents agreed wherein 6 strongly agreed. 6.7% is neutral while 26.7% disagreed. These results indicate that the majority of the respondents use torrent software other than the websites provided in the study, which are Google Drive and Mega, in order to download the paid software that they need.

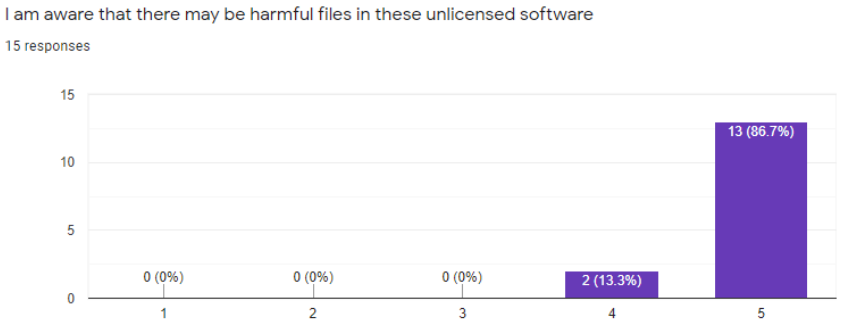

Figure 15. Bar Graph Result of Question #14

For Figure 15, the respondents were also asked if they have any certain form of awareness when it comes to harmful files that can be included in unlicensed software. All of the respondents agreed where 86.7% strongly agreed. This indicates that all the respondents are aware when it comes to harmful files that may be included in unlicensed software that can be downloaded from the internet.

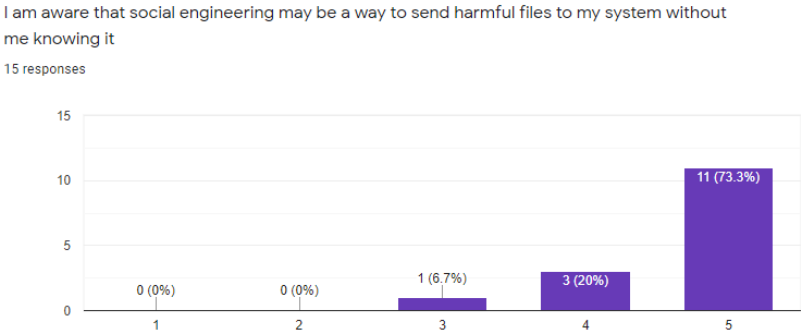

Figure 16. Bar Graph Result of Question #15

Lastly, in Figure 16, the respondents were asked if they are aware about the concept of social engineering wherein it can be a way to send harmful files to one's system without the user's knowledge. 93.3% of the respondents agreed where 73.3% strongly agreed while 6.7% is neutral. This result indicates that majority of the respondents are aware about social engineering and that they have ways to prevent this sort of attack from happening in their system.

5.3 Proposed Improvements

Given the findings, the researchers would like to recommend the following that users refrain from using unlicensed software. Unlicensed software is not secure and are prone to have malicious software due to it being exploitable and security patches are not applied. Since the methodology that this study has applied has proven that users are at risk when using unlicensed software, the researchers can safely say that it is better if users acquire installers from authorized distributors only. Second, the researchers recommend that browsers, specifically Google Chrome, improve their security features in detecting malicious files. Cloud storage services such as Google Drive and Mega's security should also be improved. This is since the results show that these services are not able to detect disguised malicious files, especially in large files, causing malicious software to bypass detection. This leads to the recommendation that Google Drive increase their maximum file size that the service is able to detect. The researchers would also recommend that antiviruses improve malicious file detection. This is based on the findings of the study where in the malicious file in .bat format avoided detection in most antivirus software. Given this, file types such as .bat is also recommended to be included in the file types to be scanned. Lastly, future researchers are recommended to further explore the study, changing variables and the scope of the study to obtain better results. Future researchers are also recommended to try different exploit methods to determine whether users are aware of these risks.

5.4 Validation

Table 2. Weighted means regarding the needs to access paid software

	WM	Verbal Interpretation
I usually need paid software and am willing to download it from the internet	3.82	Often Needs

Never needs 1.00 - 1.49 Rarely needs 1.50 – 2.49 Sometimes needs 2.50 – 3.49 Often needs 3.50 – 4.49 Always needs 4.50 – 5.00

Table 2 shows a weighted mean of 3.82, indicating that the participants often need access to paid software. In this study, the participants are all students who only often need to use the paid software application in a short amount of time.

Table 3. Weighted means regarding the use of torrent to download software

	WM	Verbal Interpretation
I use Torrent to download the software	3.8	Often Uses

Never uses 1.00 – 1.49 Rarely uses 1.50 – 2.49 Sometimes uses 2.50 – 3.49 Often uses 3.50 – 4.49 Always uses 4.50 – 5.00

Table 3 presents a weighted mean of 3.8, showing that the participants often use a torrenting software to install the cracked software they needed. Torrents are known to be highly anonymous and the torrented files sometimes include malicious codes that may cause harm to the user.

Table 4. Weighted means regarding the awareness of the risk downloading software

	WM	Verbal Interpretation
I am aware of the risk when downloading cracked software	4.77	Extremely Aware

Not at all aware 1.00 - 1.49 Slightly aware 1.50 – 2.49 Moderately aware 2.50 – 3.49 Very aware 3.50 – 4.49 Extremely aware 4.50 – 5.00

Table 4 results in an outstanding weighted mean of 4.77, revealing that the participants are extremely aware of how dangerous and risky downloading cracked software is. This shows that even if the participants knew the risks, they still try to download cracked software rather than pay an exorbitant price for a software they only need temporarily.

6. Conclusion

Based on the data collected, the researchers concluded that most of the students are prone to the vulnerability of downloading a cracked software which is the Adobe Photoshop but was injected with a malicious software. Therefore, students who are in need of computer programs with subscription fees that can be used for their school work are vulnerable to a social engineering attack. Having such findings, it was concluded that more than half of the students know how to examine and check all the files they have downloaded in the internet before installing them. Most of them also have anti-virus installed in their laptop but cannot detect the malware from the file they have downloaded. Therefore, students know some ways how to protect themselves from malicious software that are harmful for their computers.

In relation to the answer of respondents, most of the students are aware about social engineering attacks and that it is one way to send harmful files or programs to their computers without realizing that they have been compromised.

The researchers also concluded that expensive subscription fees in many computer programs that will be helpful to their school works have a great impact to them settling to cracked programs from torrents and other websites that provide software they need for free even though most of them are aware that there may be harmful files in those unlicensed or cracked software.

REFERENCES

Arli, D. and Tjiptono, F. 2016. Consumer digital piracy behaviour among youths: insights from Indonesia. Asia Pacific *Journal of Marketing and Logistics*, Vol. 28 No. 5, pp. 898-922. https://doi.org/10.1108/APJML-11-2015-0163

Kumar, S., Madhavan, L., Nagappan, M., Sikdar, B. 2016. Malware in Pirated Software: Case Study of Malware Encounters in Personal Computers. 2016 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, pp. 423-427. doi: 10.1109/ARES.2016.101.

Munasinghe, P. G. and Pemarathna. 2017. Students' Intention to Use of Pirated Software in Rajarata University of Sri Lanka. *IOSR Journal of Business and Management (IOSR-JBM)* 19.12 (2017): 52-58. DOI: 10.9790/487X-1912015258

Ullah, F. et al. 2019. Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach. *IEEE Access*, vol. 7, pp. 124379-124389. doi: 10.1109/ACCESS.2019.2937347.

Biography

Christer John M. Esguerra is a 3rd year student under the course of Bachelor of Science in Information Technology under the School of Information Technology at Mapua University - Makati, Makati, Philippines. His research interests include cybersecurity, data visualization and social engineering.

Dan Christopher Fandiño is a 3rd year student under the course of Bachelor of Science in Information Technology under the School of Information Technology at Mapua University - Makati, Makati, Philippines. His research interest includes cybersecurity, social engineering and exploits especially in simple packages that is overlooked.

Angelo Luisse Gonzales is a 3rd year student under the course of Bachelor of Science in Information Technology under the School of Information Technology at Mapua University - Makati, Makati, Philippines. His research interests include social engineering, vulnerability assessment and cybersecurity.

Bryelle Timothy C. Nisperos is a 3rd year student under the course of Bachelor of Science in Information Technology under the School of Information Technology at Mapua University - Makati, Makati, Philippines. His research interests include networking and cybersecurity specifically about pentesting.

Luis Angelo Pono is a 3rd year student under the course of Bachelor of Science in Information Technology under the School of Information Technology at Mapua University - Makati, Makati, Philippines. He is interested in research concerning cybersecurity, specifically regarding social engineering and exploits.

Eric Blancaflor is an Associate Professor of Mapua University, Philippines. He earned B.S. in Electronics Engineering from Mapua University, Masters in Engineering major in Computer Engineering in the University of the City of Manila and currently working on his dissertation study as a requirement for the degree Doctor of Technology in Technological University of the Philippines. He has published conference papers related to IT systems, network design and security.